# 轻量级分组密码算法ESF的相关密钥不可能差分分析

谢 敏* 曾琦雅

(西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)

**摘 要**：八阵图算法(ESF)是一种具有广义Feistel结构的轻量级分组密码算法，可用在物联网环境下保护射频识别(RFID)标签等资源受限的环境中，目前对该算法的安全性研究主要为不可能差分分析。该文通过深入研究S盒的特点并结合ESF密钥扩展算法的性质，研究了ESF抵抗相关密钥不可能差分攻击的能力。通过构造11轮相关密钥不可能差分区分器，在此基础上前后各扩展2轮，成功攻击15轮ESF算法。该攻击的时间复杂度为$2^{40.5}$次15轮加密，数据复杂度为$2^{61.5}$个选择明文，恢复密钥比特数为40 bit。与现有结果相比，攻击轮数提高的情况下，时间复杂度降低，数据复杂度也较为理想。

**关键词**：轻量级分组密码；ESF算法；相关密钥；不可能差分分析

**中图分类号**：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2019)05-1173-07

**DOI**: 10.11999/JEIT180576

# Related-key Impossible Differential Cryptanalysis on Lightweight Block Cipher ESF

XIE Min ZENG Qiya

(*State Key Laboratory of Integrated Services Networks*, *Xidian University*, *Xi'an* 710077, *China*)

**Abstract**: Eight-Sided Fortress (ESF) is a lightweight block cipher with a generalized Feistel structure, which can be used in resource-constrained environments such as protecting Radio Frequency IDentification (RFID) tags in the internet of things. At present, the research on the security of ESF mainly adopts the impossible differential cryptanalysis. The ability of ESF to resist the related-key impossible differential cryptanalysis is studied based on the characteristics of its S-boxes and key schedule. By constructing an 11-round related-key impossible differential distinguisher, an attack on 15-round ESF is proposed by adding 2-round at the top and 2-round at the bottom. This attack has a time complexity of $2^{40.5}$ 15-round encryptions and a data complexity of $2^{61.5}$ chosen plaintexts with 40 recovered key-bit. Compared with published results, the time complexity is decreased and the data complexity is ideal with the number of attack rounds increased.

**Key words**: Lightweight block cipher; ESF algorithm; Related-key; Impossible differential attack

## 1 引言

当前，电子信息技术迅速发展，射频识别(Radio Frequency IDentification, RFID)等技术广泛应用，为了在这些资源受限的环境中对数据进行加密需采用轻量级密码算法，因此具有占用资源少、功耗低、效率高、易于实现等优势的轻量级分组密码被提出并迅速成为研究热点，如LBlock[1], MIBS[2], PRESENT[3]等。八阵图算法(Eight-Sided Fortress, ESF)[4]是根据LBlock改进而得的一种轻量级分组密码算法，其整体结构与LBlock基本一致，但借鉴了PRESENT算法中P层置换的设计，利用按位置换的形式替换LBlock中4 bit为一组进行置换的形式，使得明文数据能经过少量轮变化后迅速扩散从而提高算法的扩散性与安全性。在安全性方面，算法提出者刘宣等人[4]给出8轮不可能差分区分器，并对11轮ESF进行了不可能差分分析；陈玉磊等人[5]利用相同的8轮区分器，通过改变轮数扩展方式以及猜测密钥的顺序，改善了11轮ESF不可能差分分析结果；高红杰等人[6]同样用文献[4]提出的8轮区分器，对12轮ESF进行了不可能差分分析；尹军等人[7,8]提

收稿日期：2018-06-11；改回日期：2018-12-19；网络出版：2018-12-26
*通信作者： 谢敏 mxie@xidian.edu.cn
基金项目：国家重点研发计划(2016YFB0800601)，国家自然科学基金委员会-通用联合基金重点项目(U1636209)，“十三五”国家密码发展基金(MMJJ20180219)

Foundation Items: The National Key Research and Development Program of China (2016YFB0800601), The Key Project of the General Joint Fund of the National Natural Science of China (U1636209), National Cryptographic Development Fund of the 13th Five-Year Plan (MMJJ20180219)

出15轮ESF差分活跃S盒的数量最少为19, 16轮ESF线性活跃S盒的数量最少为15，并用相关密钥差分分析得到11轮ESF相关密钥差分特征，在此基础上对13轮ESF进行了攻击。

本文使用的相关密钥不可能差分方法是将相关密钥分析和不可能差分分析相结合。相关密钥分析是由Knudsen[9]和Biham[10]提出的，是利用轮密钥之间的关系来恢复密钥的一种分析方法。不可能差分分析由Biham等人[11]提出，是通过差分概率为0的差分来过滤错误密钥从而恢复正确密钥的一种攻击方法，该方法应用较为广泛，对Deoxys-BC[12], SPECK[13], MIBS[14]等分组密码都有较好分析结果。通过结合这两种分析方法，可选定两个特殊的密钥差分以及明文差分使其正好抵消，致使活跃S盒个数减少且差分链长度增加，从而实现更多轮数的攻击。目前，该方法已应用于对LBlock[15], MIBS[16]等分组密码的安全性分析。本文利用相关密钥不可能差分方法研究对ESF的攻击，在现有不可能差分的结果上，加入相关密钥分析，通过构造11轮的相关密钥不可能差分区分器，成功实现对15轮ESF的相关密钥不可能差分攻击，此攻击不仅在攻击轮数上有所提高，恢复密钥比特数有所增加，而且时间复杂度大幅降低，数据复杂度也较为理想，是目前关于ESF算法安全性分析的最好结果。

论文的组织结构如下：第2节简要说明要使用的符号及ESF算法的基本知识；第3节给出11轮相关密钥不可能差分区分器的构造过程并详细说明恢复15轮ESF密钥的方法；第4节对全文进行总结。

## 2 ESF算法简介

### 2.1 符号表示和基本概念

本文常用符号约定如表1所示：

### 2.2 ESF算法简介

ESF是LBlock的改进算法，算法整体采用变体的Feistel结构，轮函数采用SPN结构。该算法分组长度和主密钥长度分别为64 bit和80 bit，采用32轮迭代。算法加密结构如图1，具体加密过程为：

(1) 输入明文$L_0||R_0$；

(2) 对$i=1,2,\cdots,31$执行：

$L_i=R_{i-1}$，

$R_i=(L_{i-1}<<<7)\oplus F(R_{i-1},K_i)$，

当$i=32$时：

$L_{32}=(L_{31}<<<7)\oplus F(R_{31},K_{32})$，

$R_{32}=R_{31}$；

(3) 输出密文$L_{32}||R_{32}$。

ESF算法轮函数$F$定义为：$F(R_j,K_j)=P(S(R_j\oplus K_j))$，计算流程如图2所示。轮函数为SPN结构，由3类基本变换组成：密钥加、混淆层以及$P$置换。

混淆层：非线性$S$函数由8个并行的S盒组成。

$P$置换：该变换为线性变换，将32 bit的$(b_{31}||b_{30}||\cdots b_1||b_0)$映射成$(c_{31}||c_{30}||\cdots c_1||c_0)$。具体

表 1 符号约定

| 符号 | 意义 |
|---|---|
| $K$ | 80 bit主密钥 |
| $K_i$ | 第$i$轮的32 bit轮密钥 |
| $K_{i,j}$ | $K_i$的第$j$个半字节 |
| $K_{i,j}^l$ | $K_{i,j}$的第$l$位 |
| $L_i$ | 第$i$轮输出密文的左边32 bit |
| $R_i$ | 第$i$轮输出密文的右边32 bit |
| $<<<7$ | 循环左移7位 |
| $\oplus$ | 按位异或运算符 |
| $\|\|$ | 二进制字符联接 |
| $[i]_2$ | 常数$i$的二进制表示 |

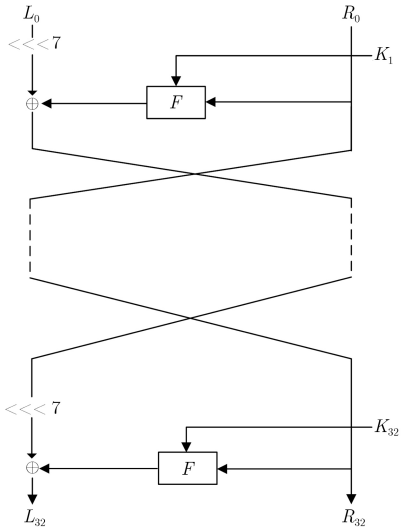


图 1 ESF算法加密流程

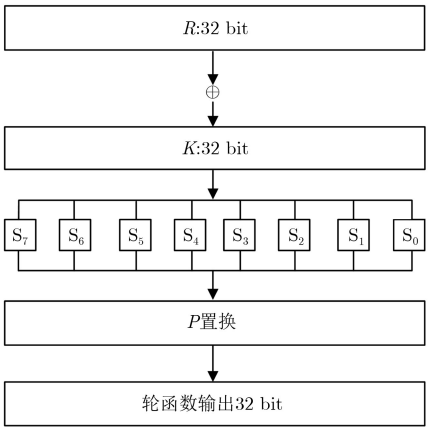


图 2 ESF算法轮函数

定义为：$(b_{31}||b_{30}||\cdots b_1||b_0)\rightarrow(c_{31}||c_{30}||\cdots c_1||c_0)$，当 $0\le i<8$ 时，$(b_{4i}||b_{4i+1}||b_{4i+2}||b_{4i+3})\rightarrow(c_i||c_{i+8}||c_{i+16}||c_{i+24})$。

### 2.3 ESF密钥扩展算法

ESF主密钥长度为80 bit，其密钥扩展算法采用了基于半字节的方式进行计算，每经过1次迭代寄存器会有13 bit更新。将$K=(k_{79}k_{78}\cdots k_1k_0)$存入寄存器，$K_1$为最左边32 bit，轮密钥更新为：

对$i=1,2,\cdots,31$，重复下列操作：

(1) $K<<<13$；

(2) $[k_{79}k_{78}k_{77}k_{76}]=S_0[k_{79}k_{78}k_{77}k_{76}]$，

$[k_{75}k_{74}k_{73}k_{72}]=S_0[k_{75}k_{74}k_{73}k_{72}]$，

$[k_{47}k_{46}k_{45}k_{44}k_{43}]=[k_{47}k_{46}k_{45}k_{44}k_{43}]\oplus[i]_2$

(3)取最左边32 bit为子密钥$K_{i+1}$。

## 3　ESF算法的相关密钥不可能差分分析

本节详细介绍15轮ESF的相关密钥不可能差分分析。首先构造11轮的相关密钥不可能差分区分器：$(00000000,00000000)\nrightarrow(00000020,00000000)$，再将此区分器向前和向后各添加2轮，实现对15轮ESF的相关密钥不可能差分攻击。

### 3.1 11轮ESF相关密钥不可能差分区分器

在实现相关密钥不可能差分攻击时，首先选择密钥差分。通过分析ESF密钥扩展算法可知：当一个非0密钥差分经过S盒后，再次经过S盒的间隔轮数较大，因此活跃S盒数量增长缓慢。在合适的地方引入非0密钥差分，不会使得每个轮密钥都有非0差分，平均连续两次出现非0密钥差分后出现4次全0密钥差分，由此可通过选定特殊的密钥差分，得到更长的密钥差分链。本文选择初始主密钥差分$\Delta K=$ (00000200000000000000)，由此构造出一条低重量密钥差分链。加解密过程用到的15轮相关密钥差分由$\Delta K$扩展而得，其中“*”表示非0半字节。扩展密钥差分如表2所示。

根据选取的密钥差分链，分别选择以$(00000000,00000000)$为第3轮输入差分、以$(00000020,00000000)$为第13轮输出差分构造相关密钥差分特征。详细的11轮ESF相关密钥不可能差分区分器如图3所示。

分析S盒的差分分布可知，当输入差分的第1个半字节为1000的数据对进入$S_1$时，该半字节的输出差分仅为1110, 0111, 1100, 1111, 1101及0110 6种可能，显然输出差分的第2位必然为非0，即图3中$b$的取值为1。则$\Delta R_{7,4}$经过S盒后的输出差分$b_1b_2b_3b_4$显然为非0，即$b_1$, $b_2$, $b_3$和$b_4$不同时为0。由$P^{-1}(\Delta L_8<<<7\oplus\Delta R_9)=P^{-1}(0000|000b\oplus f|0000|000c\oplus g|0000|000d\oplus h|0000|000a\oplus i)=(0000|0000|0000|0000|0000|0000|0000|(b\oplus f)(c\oplus g)(d\oplus h)(a\oplus i))$可知，$P^{-1}(\Delta L_8<<<7\oplus\Delta R_9)$的第1, 3, 5和7个半字节同时为0。而$S(\Delta R_8\oplus\Delta K_9)=S(0a_1e_1b_1|0c_10d_1|0a_2e_2b_2|0c_20d_2|0a_3e_3b_3|0c_30d_3|0a_4e_4b_4|0c_40d_4)$，由S盒的性质可得，当输入差分非0的半字节进入S盒时，输出差分也必然非0。因为$b_1$, $b_2$, $b_3$和$b_4$不同时为0，所以$S(\Delta R_8\oplus\Delta K_9)$的第1, 3, 5和7个半字节必然不同时为0，即$S(\Delta R_8\oplus\Delta K_9)\ne P^{-1}(\Delta L_8<<<7\oplus\Delta R_9)$。因此，加密和解密的相关密钥差分特征相遇时发生矛盾，满足相关密钥不可能差分原理。所以，上述两条概率为1的相关密钥差分路径构成了11轮的相关密钥不可能差分区分器：$(00000000,00000000\nrightarrow(00000020,00000000)$。

表 2　15轮相关密钥差分路径

| $\Delta K=$ (00000200000000000000) | | | |
|---|---|---|---|
| $\Delta K_1$ | 00000200 | $\Delta K_9$ | 00000000 |
| $\Delta K_2$ | 00400000 | $\Delta K_{10}$ | 00000000 |
| $\Delta K_3$ | 00000000 | $\Delta K_{11}$ | 00000000 |
| $\Delta K_4$ | 00000000 | $\Delta K_{12}$ | 00000000 |
| $\Delta K_5$ | 00000000 | $\Delta K_{13}$ | 00000020 |
| $\Delta K_6$ | 00000000 | $\Delta K_{14}$ | 00040000 |
| $\Delta K_7$ | 00000080 | $\Delta K_{15}$ | *0000000 |
| $\Delta K_8$ | 00100000 | – | – |

与文献[4–6]中的8轮不可能差分区分器相比，本文构造的是11轮相关密钥不可能差分区分器，其构造方法实现了前4轮向下加密迭代过程中没有差分扩散，第13轮将输入差分与密钥差分相互抵消，从而减少差分的扩散得以提高区分器的轮数，进而在一定程度上提高攻击的轮数。与文献[8]中的11轮相关密钥差分区分器相比，在区分器轮数相同的情况下，本文构造的相关密钥不可能差分区分器可实现更高轮数的攻击，恢复更多的密钥。

### 3.2 15轮ESF相关密钥不可能差分分析

运用上文构造的11轮相关密钥不可能差分区分器，向前和向后分别添加2轮，可实现对15轮ESF算法的相关密钥不可能差分分析。扩展差分路径如图4所示。

基于上述15轮ESF的相关密钥不可能差分路径，下面给出具体的攻击过程：

步骤 1　数据收集。选择$2^{24}$个明文生成一个结构，该结构包括$2^{24}\times2^{24}\times1/2=2^{47}$个明文对，其中$L_0$的第0, 2, 3, 4, 6, 8, 10, 11, 12, 14, 16, 18, 19, 20, 22, 24, 26, 27, 28, 30 bit和$R_0$的第6, 14, 22,

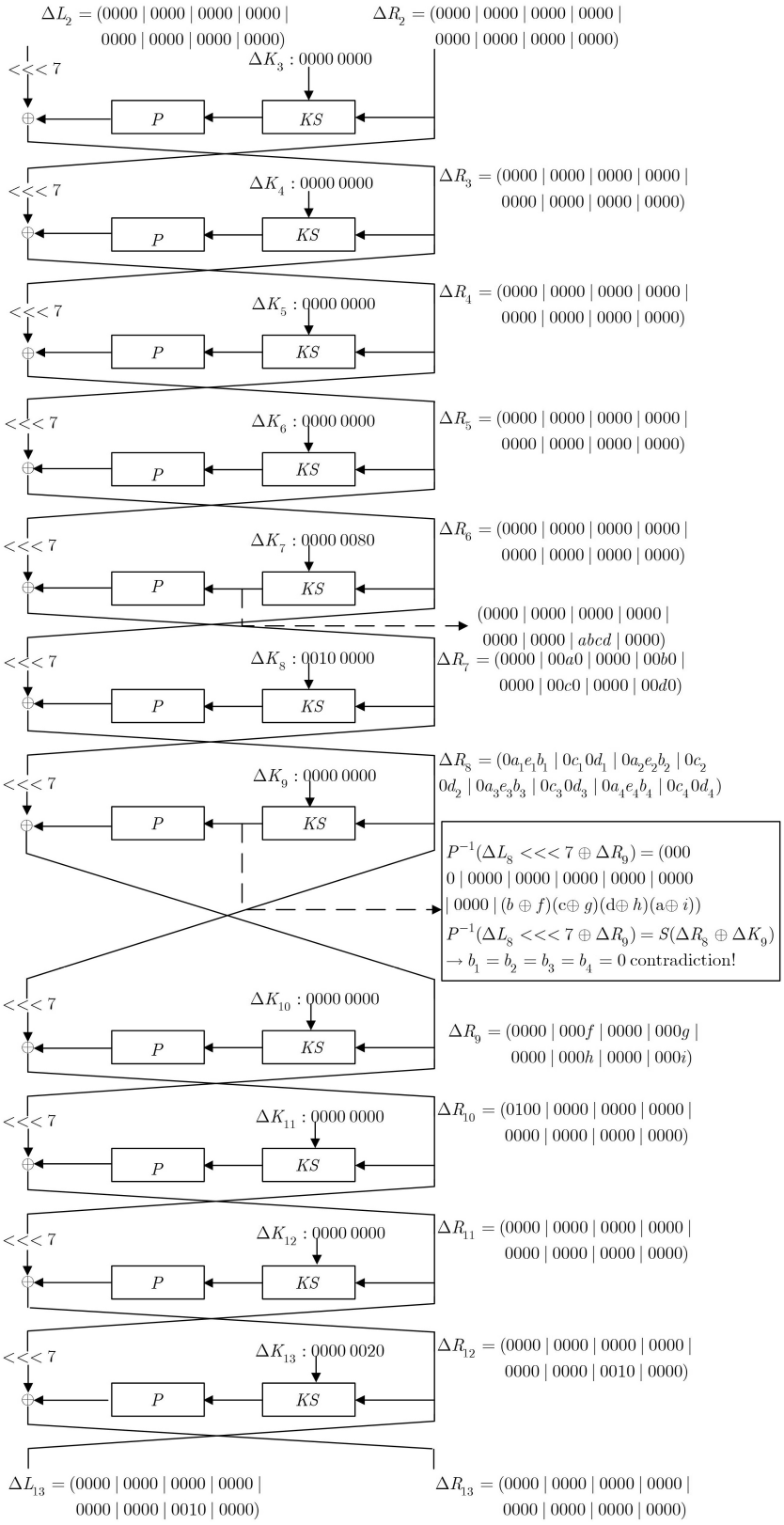


图 3 ESF算法的11轮相关密钥不可能差分区分器

30 bit可任意取值，剩下的比特取定值，即明文对满足输入差分为$(\Delta L_0, \Delta R_0) = (0j_40k_4|n_4l_40m_1|0j_10k_1|n_1l_10m_2|0j_20k_2|n_2l_20m_3|0j_30k_3|n_3l_30m_4, 0m00|0000|0j00|0000|0k00|0000|0l00|0000)$，其中$j_i$，$k_i$，$l_i$，$m_i$和$n_i(1 \le i \le 4)$遍历各种可能。选择$2^n$个这样的明文结构，则可以构成$2^{n+47}$个明文对。

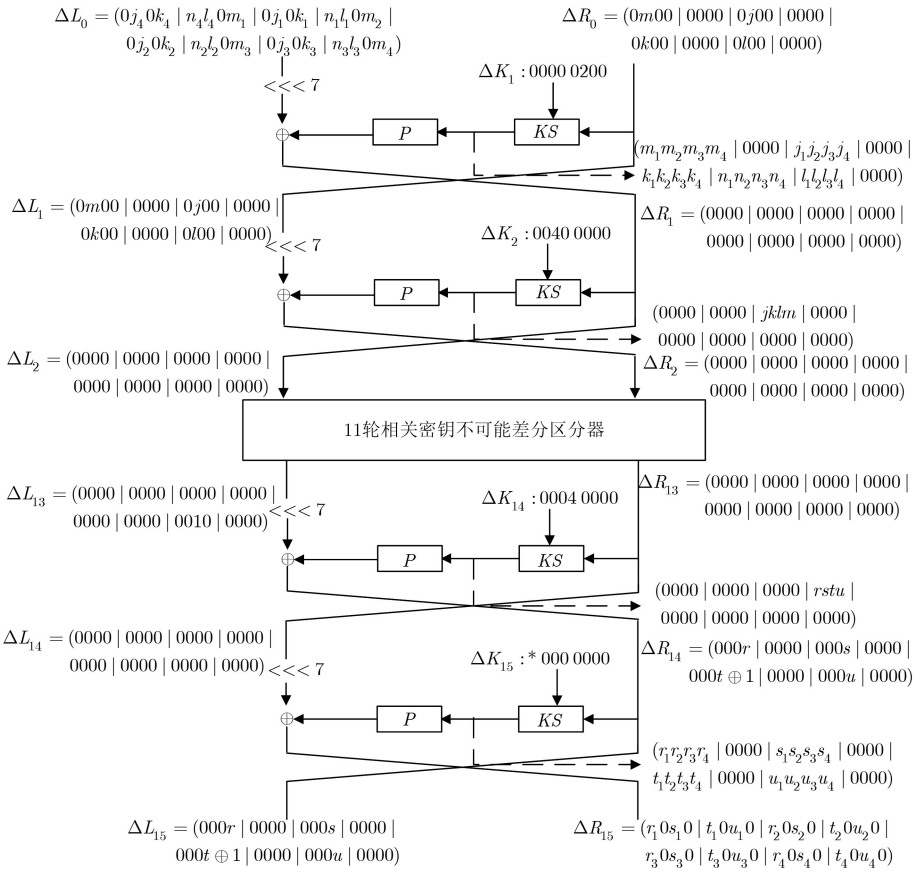


图 4 ESF算法的15轮相关密钥不可能差分路径

步骤 2　密文筛选。将选择的明文对在$\Delta K = (00000200000000000000)$的条件下加密15轮，获得对应密文对。对密文对进行排除，只保留输出差分满足$(\Delta L_{15}, \Delta R_{15}) = (000r|0000|000s|0000|000t \oplus 1|0000|000u|\ 0000, r_1 0 s_1 0|t_1 0 u_1 0|r_2 0 s_2 0|t_2 0 u_2 0|r_3 0 s_3 0|t_3 0 u_3 0|r_4 0 s_4 0|t_4 0 u_4 0)$的密文对，其中$r$, $s$, $t$, $u$, $r_j$, $s_j$, $t_j$和$u_j (1 \le j \le 4)$取所有可能的值，排除数据对后剩下的数据对个数为$2^{n+3}$。

步骤 3　依次猜测密钥$K_{15,1}$, $K_{15,3}$, $K_{15,5}$和$K_{15,7}$，共计16 bit。它们在$K$中的对应位置为$k_{33-30}$, $k_{41-38}$, $k_{49-46}$和$k_{57-54}$。对密文对进行局部解密一轮运算，保留输出差分满足等式$S_1(L_{15,1} \oplus K_{15,1}) \oplus S_1(L_{15,1} \oplus \Delta L_{15,1} \oplus K_{15,1} \oplus \Delta K_{15,1}) = \Delta R^1_{15,6} ||\Delta R^1_{15,4}||\Delta R^1_{15,2}||\Delta R^1_{15,0}$的密文对，排除不符合要求的数据对；继续检查剩余数据对的输出差分，并排除不满足等式$S_3(L_{15,3} \oplus K_{15,3}) \oplus S_3(L_{15,3} \oplus \Delta L_{15,3} \oplus K_{15,3} \oplus \Delta K_{15,3}) = \Delta R^3_{15,6}||\Delta R^3_{15,4}||\Delta R^3_{15,2}||\Delta R^3_{15,0}$的数据对。对剩余数据对检查其输出差分，排除不满足等式$S_5(L_{15,5} \oplus K_{15,5}) \oplus S_5(L_{15,5} \oplus \Delta L_{15,5} \oplus K_{15,5} \oplus \Delta K_{15,5}) = \Delta R^1_{15,7}||\Delta R^1_{15,5}||\Delta R^1_{15,3}||\Delta R^1_{15,1}$的数据对；继续检查剩余数据对的输出差分，并排除不满足等式$S_7(L_{15,7} \oplus K_{15,7}) \oplus S_7(L_{15,7} \oplus \Delta L_{15,7} \oplus K_{15,7} \oplus \Delta K_{15,7}) = \Delta R^3_{15,7}||\Delta R^3_{15,5}||\Delta R^3_{15,3}||\Delta R^3_{15,1}$的数据对。此时剩余数据对个数为$2^{n+3} \times 2^{-16} = 2^{n-13}$，该步的时间复杂度为$(2^{n+3} \times 2^4 + 2^{n-1} \times 2^8 + 2^{n-5} \times 2^{12} + 2^{n-9} \times 2^{16}) \times 1/8 \times\ 1/15 \approx 2^{n+2.09}$。

步骤 4　依次猜测密钥$K_{1,1}$, $K_{1,2}$, $K_{1,3}$, $K_{1,5}$和$K_{1,7}$。它们在$K$中的对应位置为$k_{55-52}$, $k_{59-56}$, $k_{63-60}$, $k_{71-68}$和$k_{79-76}$，由于$k_{55-54}$和$k_{57-56}$在步骤3中已猜测，所以只需要猜测余下密钥，共计16 bit。对剩余数据对部分加密1轮，依次验证下列等式是否成立：$S_1(R_{0,1} \oplus K_{1,1}) \oplus S_1(R_{0,1} \oplus \Delta R_{0,1} \oplus K_{1,1} \oplus \Delta K_{1,1}) = \Delta L^2_{0,4}||\Delta L^2_{0,2}||\Delta L^2_{0,0}\ ||\Delta L^2_{0,0} S_2(R_{0,2} \oplus K_{1,2}) \oplus S_2(R_{0,2} \oplus \Delta R_{0,2} \oplus K_{1,2} \oplus \Delta K_{1,2}) = \Delta L^3_{0,4} ||\Delta L^3_{0,2}||\Delta L^3_{0,0}||\Delta L^3_{0,6}$，$S_3(R_{0,3} \oplus K_{1,3}) \oplus S_3(\ R_{0,3} \oplus \Delta R_{0,3} \oplus K_{1,3} \oplus \Delta K_{1,3}) = \Delta L^0_{0,5}||\Delta L^0_{0,3}||\Delta L^0_{0,1}||\Delta L^0_{0,7}$，$S_5(R_{0,5} \oplus K_{1,5}) \oplus S_5(R_{0,5} \oplus \Delta R_{0,5} \oplus K_{1,5} \oplus \Delta K_{1,5}) = \Delta L^2_{0,5}||\Delta L^2_{0,3}||\Delta L^2_{0,1}||\Delta L^2_{0,7}$，$S_7(R_{0,7} \oplus K_{1,7}) \oplus S_7(R_{0,7} \oplus \Delta R_{0,7} \oplus K_{1,7} \oplus \Delta K_{1,7}) = \Delta L^0_{0,6}||\Delta L^0_{0,4}||\Delta L^0_{0,2}||\Delta L^0_{0,0}$。排除不满足以上所有等式的数据对，此时剩余数据对个数为$2^{n-13} \times 2^{-20} = 2^{n-33}$，该步的时间复杂度为：$(2^{n-13} \times 2^{18} + 2^{n-17} \times 2^{20} + 2^{n-21} \times$

$2^{24}+2^{n-25}\times 2^{28}+2^{n-29}\times 2^{32})\times 1/8\times 1/15\approx 2^{n-0.91}$。

步骤 5 猜测密钥$K_{2,5}$，$K_{1,4}$，$K_{1,5}$，$K_{1,6}$和$K_{1,7}$。它们在$K$中的对应位置为$k_{58-55}$，$k_{67-64}$，$k_{71-68}$，$k_{75-72}$和$k_{79-76}$，由于$k_{58-55}$，$k_{71-68}$和$k_{79-76}$在上述步骤中已被猜测，所以该步仅需要猜测余下的8 bit。对余下数据对进行局部加密两轮操作，检查其输出差分，并排除不满足等式$S_5(R_{1,5}\oplus K_{2,5})\oplus S_5(R_{1,5}\oplus\Delta R_{1,5}\oplus K_{2,5}\oplus\Delta K_{2,5})=\Delta L^2_{1,5}||\Delta L^2_{1,3}||\Delta L^2_{1,1}||\Delta L^2_{1,7}$的数据对，其中$R^3_{1,5}=S^2_7(R_{0,7}\oplus K_{1,7})\oplus L^0_{0,4}$，$R^2_{1,5}=S^2_6(R_{0,6}\oplus K_{1,6})\oplus L^3_{0,3}$，$R^1_{1,5}=S^2_5(R_{0,5}\oplus K_{1,5})\oplus L^2_{0,3}$，$R^0_{1,5}=S^2_4(R_{0,4}\oplus K_{1,4})\oplus L^1_{0,3}$。此时剩余数据对个数为$2^{n-33}\times 2^{-4}=2^{n-37}$，该步的时间复杂度为：$2^{n-33}\times 2^{40}\times 2/8\times 1/15\approx 2^{n+1.09}$。

步骤 6 猜测$R_{13,4}$的值，总共$2^4$种可能。进行局部解密两轮，保留满足$F(\Delta R_{13,4}\oplus\Delta K_{14,4})\oplus(\Delta L^0_{15,7}||\Delta L^0_{15,5}||\Delta L^0_{15,3}||\Delta L^0_{15,1})=(0010)$的数据对。由$S_4$的差分分布表知，满足第14轮输出要求的概率为1/6，则此步之后剩余数据对个数为$2^{n-37}\times 2^4\times 1/6\approx 2^{n-35.58}$，该步的时间复杂度为：$2^{n-37}\times 2^4\times 2^{40}\times 1/8\times 1/15\approx 2^{n+0.09}$。选择$2^{37.5}$个明文结构，即取$n=37.5$，经上述步骤过滤后，还有剩余的数据对，表明以上猜测满足了该相关密钥不可能差分路径，从而是错误密钥，需将其剔除并重新猜测密钥。因此该攻击的时间复杂度为：$2^{n+2.09}+2^{n-0.91}+2^{n+1.09}+2^{n+0.09}\approx 2^{n+3}=2^{40.5}$次15轮加密运算，明文量为：$2^{37.5+24}=2^{61.5}$个选择明文。

综上，本文采用相关密钥不可能差分分析15轮ESF的时间复杂度约为$2^{40.5}$次15轮加密操作，数据复杂度为$2^{61.5}$个选择明文，总共恢复40 bit密钥。

### 3.3 结果对比

目前对ESF的攻击最常用的方法为不可能差分分析，还有少量评估ESF在差分故障攻击与相关密钥差分攻击下的安全性的文献。本文评估了ESF抵抗相关密钥不可能差分分析能力，与现有攻击结果相比，首次将攻击轮数提高到15轮，比目前最好结果提高两轮，并且攻击时间复杂度大幅度降低，恢复的密钥比特数也具有较大优势，均优于文献[4–6,8]的结果，具体攻击结果对比如表3所示。

**表 3 ESF算法的攻击结果比较**

| 攻击方法 | 轮数 | 时间复杂度 | 数据复杂度 | 文献 |
|---|---|---|---|---|
| 不可能差分 | 11 | $2^{75.5}$ | $2^{59}$ | [4] |
| 不可能差分 | 11 | $2^{32}$ | $2^{53}$ | [5] |
| 不可能差分 | 12 | $2^{60.43}$ | $2^{53}$ | [6] |
| 相关密钥差分 | 13 | $2^{66}$ | $2^{47}$ | [8] |
| 相关密钥不可能差分 | 15 | $2^{40.5}$ | $2^{61.5}$ | 本文 |

## 4 结束语

本文通过分析ESF的密钥扩展算法的弱点、S盒的差分性质以及相关密钥不可能差分分析方法的优点，以减少活跃S盒的数量来获取更长的差分链为基本思想，选定特殊的密钥和明文差分使其互相抵消，构造出11轮相关密钥不可能差分区分器，并将其前后各添加两轮，对ESF进行了15轮相关密钥不可能差分攻击，其攻击的时间复杂度远低于穷举攻击的复杂度，攻击效果与现有结果相比也具有较大优势。将多种分析方法相结合可以充分利用各种分析方法的优势，取长补短，有利于攻击更高轮数的算法，获得更加理想的攻击结果。在未来的工作中，可考虑对路径搜索算法加以优化，寻找更好的相关密钥不可能差分路径来改善目前已有的结果，或将相关密钥不可能差分分析与其他分析方法相结合，以期完成对更高轮数的ESF算法分析。

## 参 考 文 献


[1] WU Wenling and ZHANG Lei. LBlock: A lightweight block cipher[C]. Proceedings of 9th International Conference on Applied Cryptography and Network Security, Nerja, Spain, 2011: 327–344. doi: 10.1007/978-3-642-21554-4_19.

[2] IZADI M, SADEGHIYAN B, SADEGHIAN S, *et al*. MIBS: A new light-weight block cipher[C]. Proceedings of CANS 2009, Ishikawa, Japan, 2009: 334–348. doi: 10.1007/978-3-642-10433-6_22.

[3] BOGDANOV A, KNUDSEN L, LEANDER G, *et al*. PRESENT: An ultra-lightweight block cipher[C]. Proceedings of Cryptographic Hardware and Embedded Systems, Vienna, Austria, 2007: 450–466. doi: 10.1007/978-3-540-74735-2_31.

[4] 刘宣, 刘枫, 孟帅. 轻量级分组密码算法ESF的不可能差分分析[J]. 计算机工程与科学, 2013, 35(9): 89–95. doi: 10.3969/j.issn.1007-130X.2013.09.014.

LIU Xuan, LIU Feng, and MENG Shuai. Impossible differential cryptanalysis of lightweight block ciper ESF[J]. *Computer and Engineering Science*, 2013, 35(9): 89–95. doi: 10.3969/j.issn.1007-130X.2013.09.014.

[5] 陈玉磊, 卫宏儒. ESF算法的不可能差分密码分析[J]. 计算机科学, 2016, 43(8): 89–91. doi: 10.11896/j.issn.1002-137X.2016.8.018.

CHEN Yulei and WEI Hongru. Impossible differential cryptanalysis of ESF[J]. *Computer Science*, 2016, 43(8): 89–91. doi: 10.11896/j.issn.1002-137X.2016.8.018.

[6] 高红杰, 卫宏儒. 用不可能差分法分析12轮ESF算法[J]. 计算机科学, 2017, 44(8): 147–150. doi: 10.11896/j.issn.1002-137X.2017.10.028.

GAO Hongjie and WEI Hongru. Impossible differential

attack on 12-round block cipher ESF[J]. *Computer Science*, 2017, 44(8): 147–150. doi: 10.11896/j.issn.1002-137X.2017.10.028.

[7] 尹军, 马楚炎, 宋健, 等. 轻量级分组密码算法ESF的安全性分析[J]. 计算机研究与发展, 2017, 54(10): 2224–2231. doi: 10.7544/issn1000-1239.2017.20170455.
YIN Jun, MA Chuyan, SONG Jian, *et al*. Security analysis of lightweight block cipher ESF[J]. *Journal of Computer Research and Development*, 2017, 54(10): 2224–2231. doi: 10.7544/issn1000-1239.2017.20170455.

[8] 尹军, 宋健, 曾光, 等. 轻量级分组密码算法ESF的相关密钥差分分析[J]. 密码学报, 2017, 4(4): 333–344. doi: 10.13868/j.cnki.jcr.000186.
YIN Jun, SONG Jian, ZENG Guang, *et al*. Related-key differential attack on lightweight block cipher ESF[J]. *Journal of Cryptologic Research*, 2017, 4(4): 333–344. doi: 10.13868/j.cnki.jcr.000186.

[9] KNUDSEN L. Crypatanalysis of LOKI[C] Proceedings of Advances in Cryptology, Gold Coast, Australia, 1991: 22–35.

[10] BIHAM E. New types of cryptanalytic attacks using related keys[J]. *Journal of Cryptology*, 1994, 7(4): 229–246. doi: 10.1007/BF00203965.

[11] BIHAM E, BIRYUKOV A, and SHAMIR A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials[C]. Proceedings of Advances in Cryptolog EUROCRYPT'99. Prague, CZ, 1999: 12–23. doi: 10.1007/3-540-48910-x_2.

[12] JIANG Zilong and JIN Chenhui. Impossible differential cryptanalysis of 8-round Deoxys-BC-256[J]. *IEEE Access*, 2018, 6: 8890–8895. doi: 10.1109/ACCESS.2018.2808484.

[13] 徐洪, 苏鹏晖, 戚文峰. 减轮SPECK算法的不可能差分分析[J]. 电子与信息学报, 2017, 39(10): 2479–2486. doi: 10.11999/JEIT170049.
XU Hong, SU Penghui, and QI Wenfeng. Impossible differential cryptanalysis of reduced-round SPECK[J]. *Journal of Electronics & Information Technology*, 2017, 39(10): 2479–2486. doi: 10.11999/JEIT170049.

[14] 付立仕, 金晨辉. MIBS-80的13轮不可能差分分析[J]. 电子与信息学报, 2016, 38(4): 848–855. doi: 10.11999/JEIT150673.
FU Lishi and JIN Chenhui. Impossible differential cryptanalysis on 13-round MIBS-80[J]. *Journal of Electronics & Information Technology*, 2016, 38(4): 848–855. doi: 10.11999/JEIT150673.

[15] XIE Min, LI Jingjing, and ZANG Yuechuan. Related-key impossible differential cryptanalysis of LBlock[J]. *Chinese Journal of Electronics*, 2017, 26(1): 35–41. doi: 10.1049/cje.2016.06.031.

[16] CHENG Lu, XU Peng, and WEI Yuechuan. New related-key impossible differential attack on MIBS-80[C]. Proceedings of 2016 International Conference on Intelligent Networking and Collaborative Systems, Ostrawva, CZ, 2016: 203–206. doi: 10.1109/incos.2016.41.

谢　敏：女，1976年生，副教授，研究方向为编码和密码.
曾琦雅：女，1993年生，硕士，研究方向为分组密码算法分析.